The Director of Central Intelligence
Washington, D.C. 20505

5 August 1986

Dear David,

Thanks very much for sending me your piece on "Year of the Spy." I think it is a very good job and a very important contribution to put the whole thing in context. As you say, we caught some nine spies, and much of the damage is temporary, while the way they were caught, in most cases, attributes to our intelligence or a reflection of the deficiency in the Soviet system. At the same time, there have been a hundred leaks which I believe have caused more permanent damage.

It was thoughtful of you to send your valuable piece and I appreciate it.

Yours,

Bill

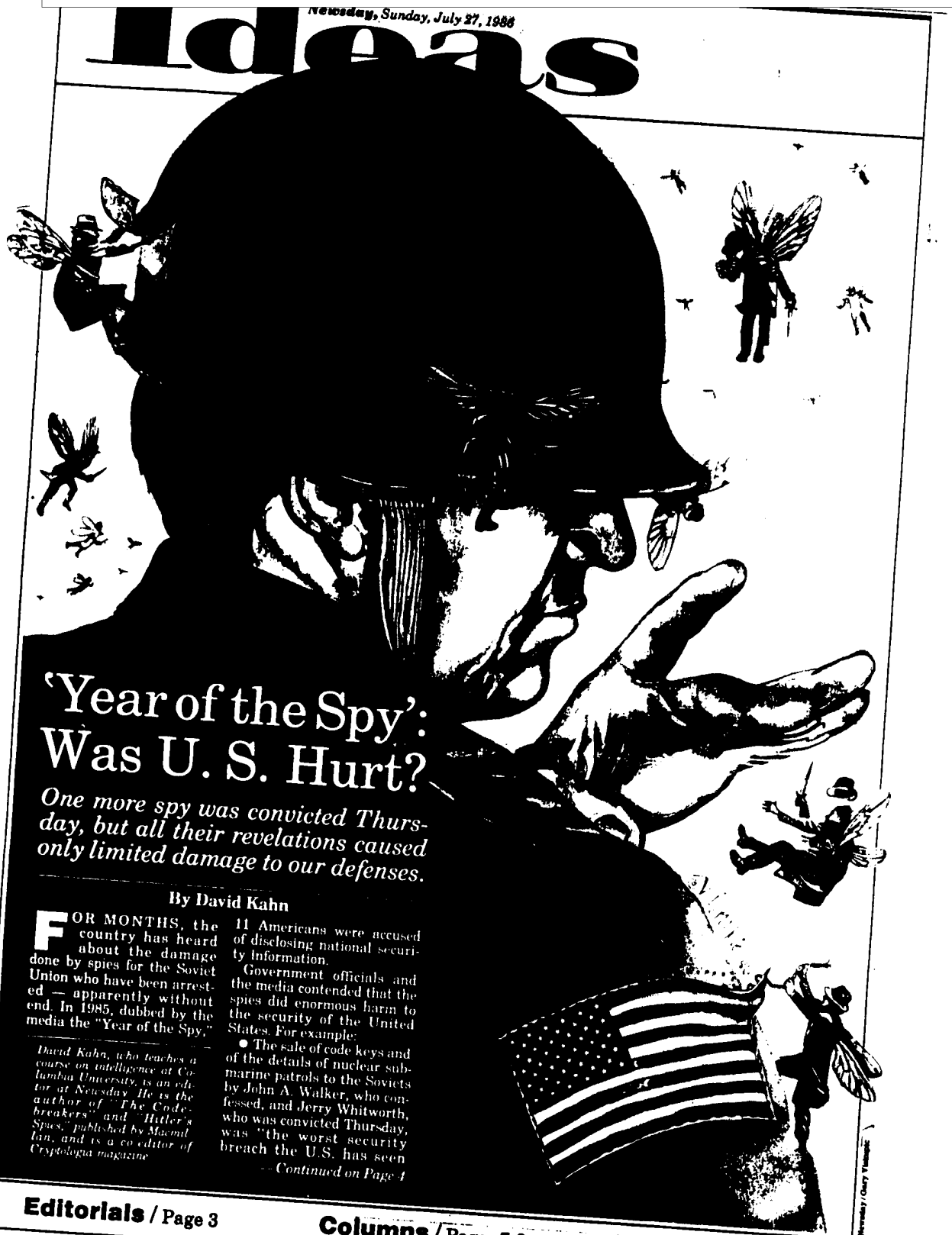
William J. Casey

Mr. David Kahn
NEWSDAY Magazine for Long Island
Long Island, New York 11747

Next 1 Page(s) In Document Denied

Newsday, Sunday, July 27, 1986

Ideas



'Year of the Spy': Was U. S. Hurt?

One more spy was convicted Thursday, but all their revelations caused only limited damage to our defenses.

By David Kahn

FOR MONTHS, the country has heard about the damage done by spies for the Soviet Union who have been arrested — apparently without end. In 1985, dubbed by the media the "Year of the Spy," 11 Americans were accused of disclosing national security information.

Government officials and the media contended that the spies did enormous harm to the security of the United States. For example:

- The sale of code keys and of the details of nuclear submarine patrols to the Soviets by John A. Walker, who confessed, and Jerry Whitworth, who was convicted Thursday, was "the worst security breach the U.S. has seen

— Continued on Page 4

David Kahn, who teaches a course on intelligence at Columbia University, is an editor at Newsday. He is the author of "The Codebreakers" and "Hitler's Spies," published by Macmillan, and is a co-editor of Cryptologia magazine.

Newsday / Gary Friedman

NEWSDAY
27 July 1986

'Year of the Spy': Was U. S. Hurt?

One more spy was convicted Thursday, but all their revelations caused only limited damage to our defenses.

By David Kahn

FOR MONTHS, the country has heard about the damage done by spies for the Soviet Union who have been arrested — apparently without end. In 1985, dubbed by the media the "Year of the Spy," 11 Americans were accused of disclosing national security information.

Government officials and the media contended that the spies did enormous harm to the security of the United States. For example:

- The sale of code keys and of the details of nuclear submarine patrols to the Soviets by John A. Walker, who confessed, and Jerry Whitworth, who was convicted Thursday, was "the worst security breach the U.S. has seen since World War II," said the U.S. attorney whose office prosecuted Whitworth. Time magazine seconded this: It was "the most damaging spy operation in the U.S. in nearly four decades."
- The disclosure by a former Central Intelligence Agency employee of the names of Soviet citizens spying for the United States — at least one of whom appears to have been executed — was "the worst intelligence loss in years," according to one informed official.
- "You cannot possibly overstate" the harm Ronald Pelton did in selling secrets of the codebreaking National Security Agency to the USSR, one former senior intelligence officer said.
- Pelton's revelations were "the worst compromise of U.S. intelligence in recent history — at least, the worst we know about," contended The Washington Times.
- Government officials called the Walker-Whitworth episode — in a climax of the litany of hyperbole — "the most damaging case of espionage in U.S. history."

Discounting the contradictions among the statements and even the exaggeration of a prosecutor seeking a conviction, how serious *were* the spy losses?

They cannot be quantified, but they are nowhere near as damaging as the shrill tone of many of the official and press statements suggests. The losses were discommoding, and expensive, but they hardly affected American power, American policies, or American ability to operate effectively in the world.

Take the alleged cryptographic disclosures of Walker, a former Navy chief warrant officer, and his friend Whitworth, a former radioman. Walker said he sold to the Soviets — in 30 installments between 1968 and 1985 — material concerning the KL-47, KW-7, KWR-37, KY-8, and KG-14 cryptographic systems. Some had been supplied by Whitworth, some Walker photographed with a tiny Minox camera, he said.

How much damage could be done by such revelations to the Soviets? Code systems have built-in safeguards which limit it.

Since the Renaissance, many cryptographic systems have consisted of two parts: the "method" and the "keys." The method is permanent and, in today's systems, is often embodied in the electrical circuits of a cipher machine. The keys, which set or program the machine, change frequently; different keys are given to different users.

Both method and keys are needed to encode, and the receiver must likewise have the method and the proper keys to decode.

In 1883, French cryptographer Auguste Kerckhoffs enunciated a fundamental goal for cryptosystems: If an enemy does not have the keys used to encode a particular cryptogram, he will not be able to solve the cryptogram, even if he knows the method. It took until the 1920s to create ciphering mechaniams that achieved this result.

Walker said under oath at Whitworth's trial that he gave the Soviets technical manuals for several of the cryptosystems. A retired NSA official testified that this would enable the Soviets to reconstruct the method of those systems. Walker further said that he gave the Soviets photographs of keys for some of these systems.

It is altogether probable that the Soviet Union utilized the technical manuals to reconstruct the cryptosystems and then applied the keys to decipher American messages that it had intercepted and preserved. But even at that, it would be able to read only messages for which it knew the method *and* had the keys.

"We design our systems," testified the NSA official, "that, without a key, we are highly confident that no one can read these communications."

The Soviet Union would have the keys only for a relatively small number of messages. The reason? Different U.S. Navy commands or regions have different keys. The western Pacific area does not have the same keys as the eastern Pacific; a carrier battle force commander holds higher level keys than a destroyer captain, though they would have some keys in common.

This multiplicity reduces damage if a key is captured, betrayed or stolen, and it keeps information from persons not intended to know it. There are "hundreds" of cryptographic nets, each of which use the same method and keys, the NSA official said. And though Walker and Whitworth had long and extensive access to Navy cryptosystems, they could not have obtained the keys to all of them.

For example, Walker testified that among the cryptographic keys he sold to the Soviet Union were those for the primary broadcast channel of the American Atlantic submarine fleet. He said nothing about the Pacific submarines, and it may therefore be presumed that the Soviets got no keys to this channel and so were excluded from reading messages on it.

STAT

Again, the Soviets were sold keys for the KWR-37 code systems for encipherment of messages sent over the western Pacific fleet broadcast channel, Walker testified. But these widely disseminated communications do not rise above "secret" in the security classification — they include no "top secret" messages — and, as Adm. Stansfield Turner, a former Central Intelligence Agency director who once commanded the Mediterranean forces of the North Atlantic Treaty Organization, said, "The stuff on the fleet broadcast is of very little significance."

All of this adds up to the fact that the cryptographic exposures by Walker and Whitworth did not jeopardize all Navy communications but were limited in scope and so in damage.

The same may be said about revelations of actual naval operations. Walker is alleged to have disclosed the duration, routing, depths and hovering points of U.S. nuclear submarine patrols as well as details of American antisubmarine warfare techniques.

This information may have helped the USSR to track and — in case of war — would have helped it to nullify our subs, the third leg of our nuclear defense triad, while pre-

2

venting many of its own submarines from being destroyed. And the Soviets might have learned, via some of the keys Whitworth is said to have supplied, details about a fleet exercise, Fltex 83-1, carried out in 1983 400 miles east of Siberia's Kamchatka Peninsula.

These details, a Navy captain testified at the Whitworth trial, consisted of an operations general order, specifics of the exercise and the Third Fleet commander's views on the exercise. Another report provided "very good insight into how the United States Navy would conduct anti-air warfare."

The captain said that an American evaluation of a similar Soviet exercise would take some 50 man-years of effort and noted that if, in addition to visual observation of the ship movements, "you have all the boilerplate of the exercise, the purpose, the tactics and the wrap-up of how the opposing force thinks they've done, you've got to save just an incalculable amount of manpower."

He also remarked that "because most navies tend to practice in peacetime the way they expect to operate in conflict," knowledge of the fleet exercise would tell the Soviet Union what to expect in case of war.

But there has been no war. The information about both surface and submarine tactics is already obsolescent and is growing increasingly so as technology evolves.

"A good deal of that [damage presumably done by Walker] fortunately has been ameliorated by time," said Adm. Bobby R. Inman, a former deputy director of the CIA and a former director of naval intelligence.

In a similar view, lots of reasons [aside from the Walker information] why the Soviets could have quieted their subs [to hamper anti-submarine warfare efforts]. I have felt that the Walker case is not as serious as people have claimed."

Turner remarked that "There are

From the Whitworth revelations about operation Fltex 83-1, the Soviets "learned some things about our fleet," Turner said. "But peacetime fleet activities aren't very important," he said, in effect contradicting the navy captain's testimony. "The Soviets won't come away with a great advantage. Since nothing serious happened when they read our codes, it [the Whitworth betrayal] is not a long-term loss."

In the political realm, a State Department arms control official said that he has seen no new Soviet strengths attributable to their new information. The reason, he believes, is that any gains in intelligence have been overshadowed by political events wholly unrelated to intelligence.

Even Soviet leader Mikhail Gorbachev's frequent and dramatic arms control proposals, so different from the stolid methods of his predecessors, stem from his way of doing things, not from any new intelligence he may have gained.

If the Walker and Whitworth revelations gave away information on U.S. military strength and operations, those of Pelton and former CIA employee Edward L. Howard deprived the United States of incoming intelligence.

Pelton was a $24,000-a-year analyst for the NSA who was found guilty of selling to the Soviet Union information on how the NSA eavesdrops on them.

An NSA official testified at Pelton's trial that Pelton's information had caused the Soviets to stop using some channels, depriving the United States of valuable data.

The United States was said to have lost still more intelligence when Howard told the KGB the names of CIA spy handlers working in Moscow and perhaps the identity of one spy, a Russian aviation engineer who was reported executed. The betrayal has left U.S. intelligence operations in Moscow "in shambles," according an intelligence official.

Did these losses hurt American policy? Did the decline in information from within the Soviet Union or about its submarines restrict American activities throughout the world or hamper the United States at the negotiating table? There seems no evidence that it has. Indeed, merely to ask whether the spy losses have altered President Ronald Reagan's methods of dealing with the Soviet Union is to show the absurdity of the idea.

Moreover, the losses will be made good. After Pelton's disclosure led the Soviet Union to stop using certain channels for sensitive information, the National Security Agency unquestionably detected this diminution and moved to seek the information, or similar information, elsewhere. It has done this time and again, as a consequence not of betrayals, but of new technology.

Other countries have repeatedly put new cryptosystems, new methods of transmission into service. But the agency has kept pace with new methods of interception and analysis, so that the loss was, in many cases, only temporary.

For example, several years after two NSA cryptanalysts defected, another ex-NSA employee said no one complained to him that their disclosures had reduced agency intelligence, indicating that the losses had been made good.

The other intelligence agencies must be doing this as well — or they're not doing the job for which they're being paid. The loss of incoming intelligence, in other words, has at most cost the United States time, money, manpower; it has not crippled our defenses.

So why did U.S. officials squeal so loudly about the losses? Was it a cynical bid to get more money to repair the damage? Neither Paul Seabury, a professor of international relations at Berkeley and until October a member of the President's Foreign Intelligence Advisory Board, nor Turner think so.

"I don't think you can overestimate how concerned these intelligence types are about any secrets coming out and how shallow they are about the consequences," Turner said. "They're not having any trouble with the budget now anyway."

And Seabury noted that when the board questioned the agencies about their work, their officials had not used the intelligence losses as an excuse for not having done better.

The exaggerations of officials seem rooted in part in the pain the damage caused. The losses mean extra work on the part of intelligence officials. Nobody likes this.

The exaggerations also seem rooted in part in a typical American ignorance of history. To call the Walker-Whitworth or the Pelton disclosures "the worst since World War II" is to blind oneself to much more serious cases since then:

- Klaus Fuchs and David Greenglass, the atomic spies, who gave nuclear secrets to the Soviets.
- Christopher Boyce and Andrew Daulton Lee, "the Falcon and the Snowman," who sold details of the Rhyolite series of satellites.
- William Kampiles, the CIA employee who sold the Soviet Union the operations manual for the new KH-11 satellite. The manual revealed that the satellite televised its extremely high-resolution pictures to the United States immediately after they were taken.

So if the damages of the Year of the Spy are seen in perspective, they do not turn out to be the awful defeats that the yelps of the officials and the media suggest. They are temporary and relatively insignificant setbacks that make the United States spend more money but do not much wound its military strength.

They in no serious way undermine the nation's security. America can sleep soundly tonight.

David Kahn, who teaches a course on intelligence at Columbia University, is an editor at Newsday. He is the author of "The Codebreakers" and "Hitler's Spies," published by Macmillan, and is a co-editor of Cryptologia magazine.